Distributed Control Systems and Resiliency

Trung Tran

9th International Symposium on Resilient Control Systems

August 17, 2016

Agenda

- Control systems are changing
  - Moving to fully distributed networks and embracing the Internet of Things (IoT)
  - Moving from cloud to edge analytics
  - Moving beyond traditional ideas of resiliency
- DARPA is investing in these areas
  - Making sensing ubiquitous and smart
  - Low-power processing to enable edge analytics
  - Securing the IoT
- DARPA would like to work with you

Control systems are evolving: a look at the past

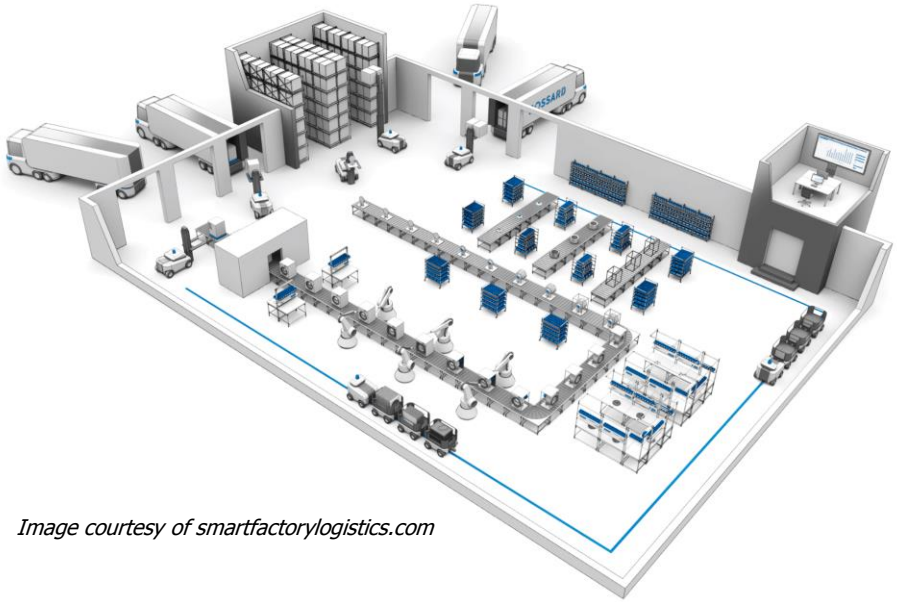


Image courtesy of smartfactorylogistics.com

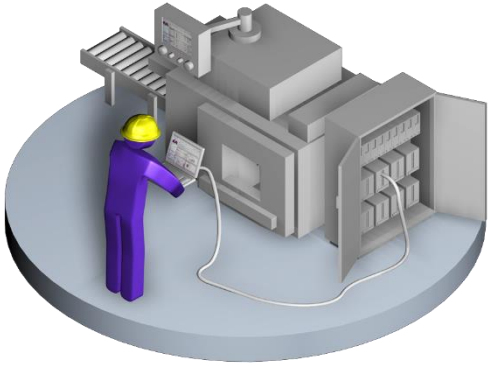


Image courtesy of grantek.com

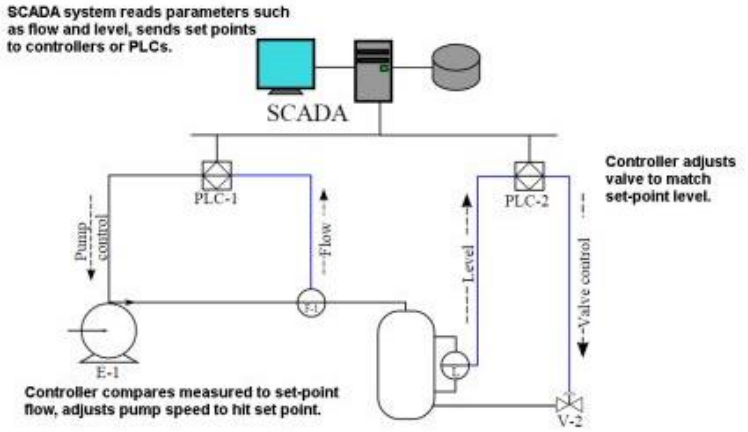
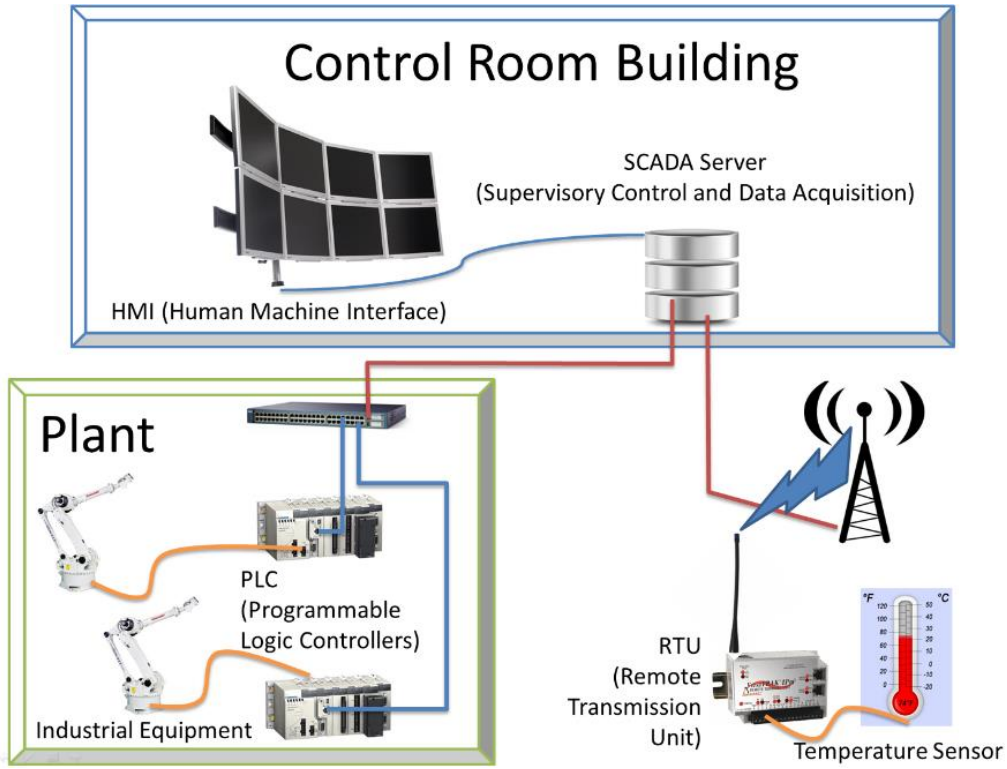


Image courtesy of www.technocratautomation.net

Control Systems:

- Self-contained within a local area
- Physically repairable
- Resiliency meant:
  - Mitigating failures to ensure uptime and safety
- Sensor and control on the same network

Control systems are now distributed



Control network

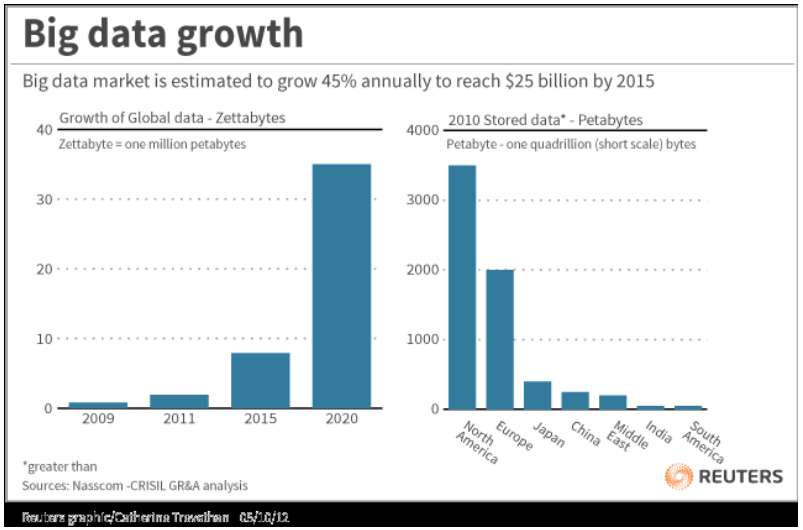
Sensor network

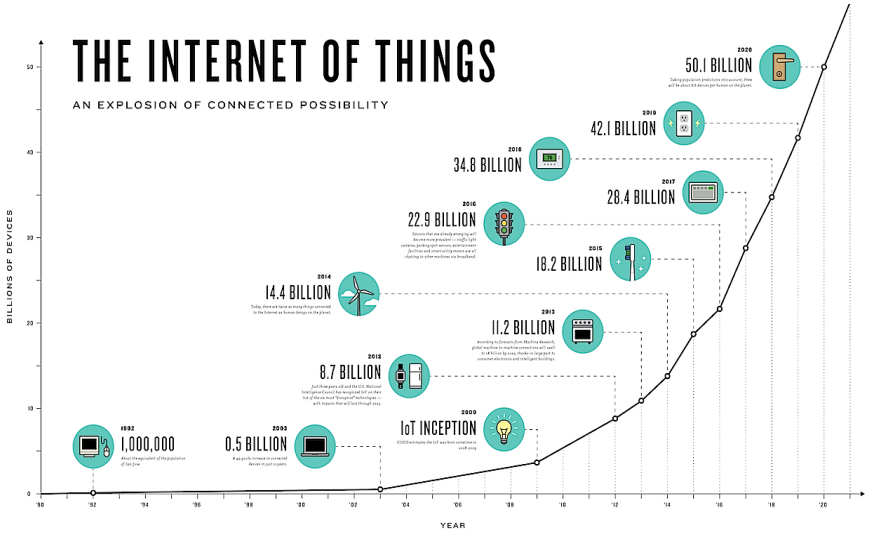
Control Systems = IoT networks

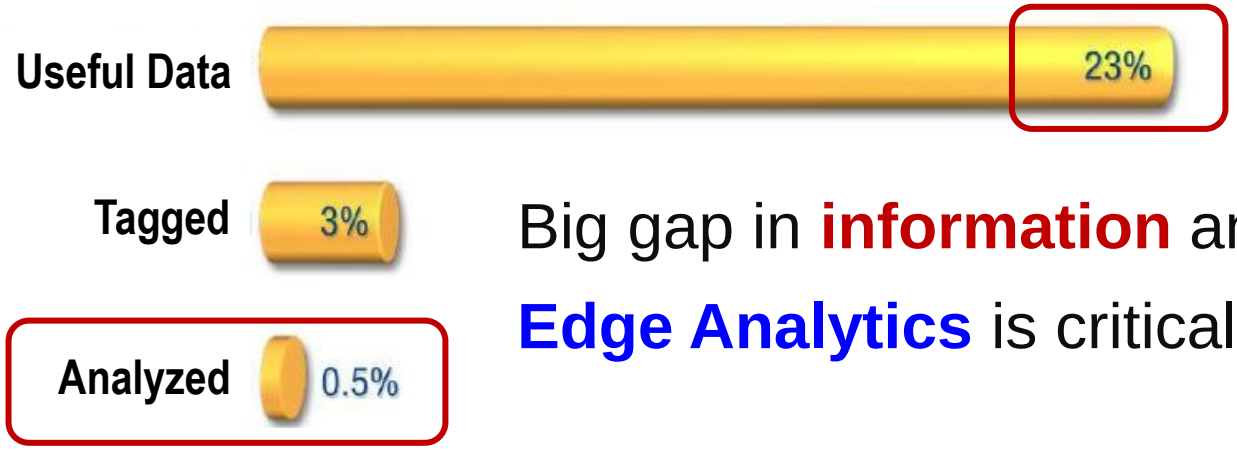
- Remotely repairable
- Resiliency still means:
  - Mitigating failures to ensure uptime and safety
- Control is done in the cloud at the center of the network

"Things"

The Era of Big (Wasted) Data





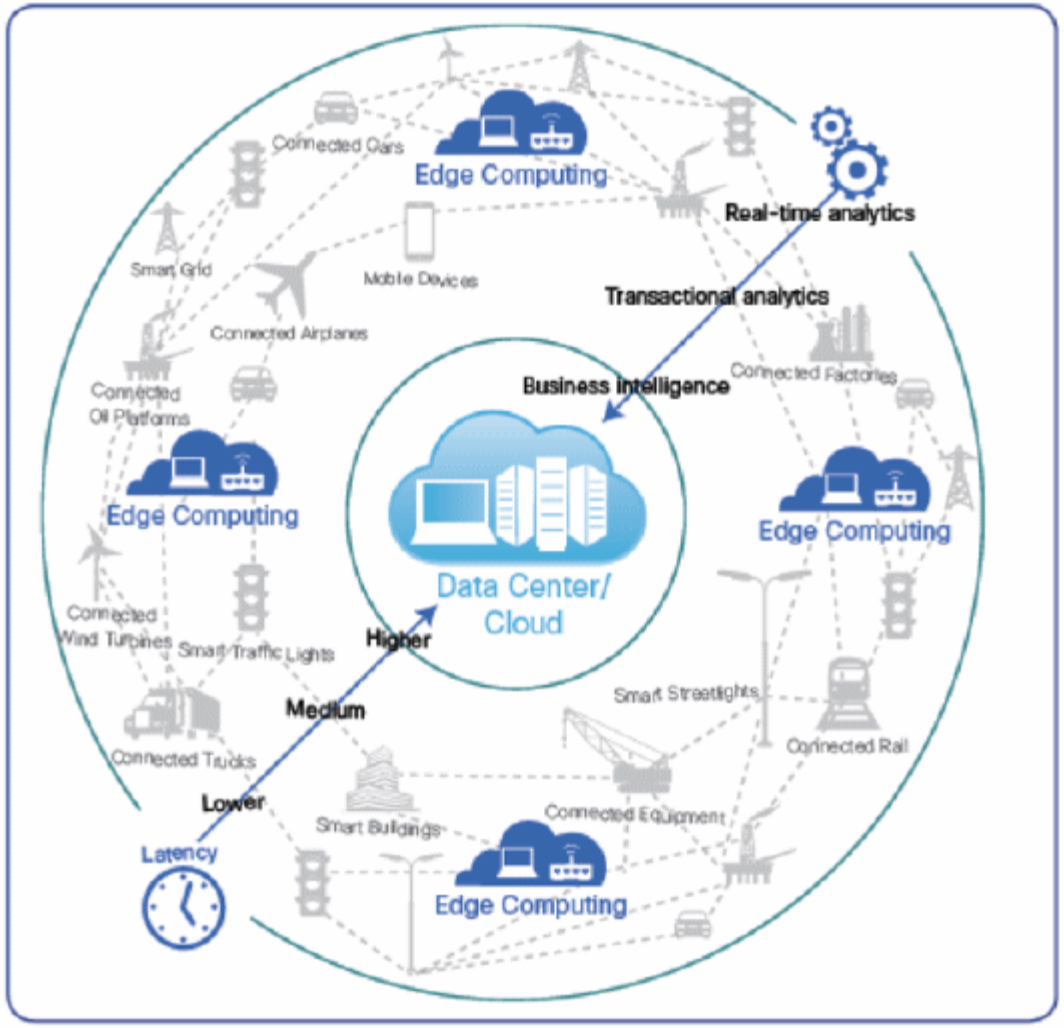


Big gap in **information** analytics!

Edge Analytics is critical

[M. Horowitz, et al., CPU DB; IDC, 2012]

Edge Analytics and Edge Computing



Source: Cisco, 2014

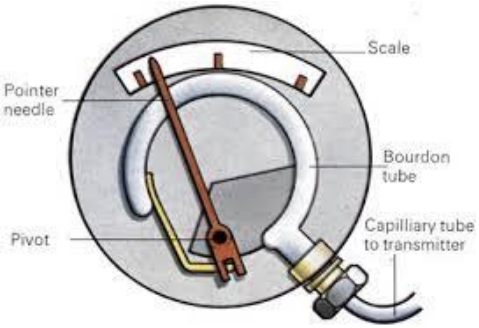
More computing at the edge

- Localized decision making
- Higher level processing
- Smaller power budgets
- Smaller form factors

"Smart" and connected is not without cost

"Dumb" sensor

Failure = wrong reading



Mechanical Failure
Fix or replace the gauge

"Smart" sensor

Failure = wrong reading

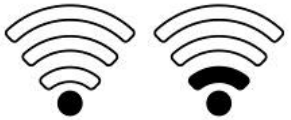
Software bugs

Malware

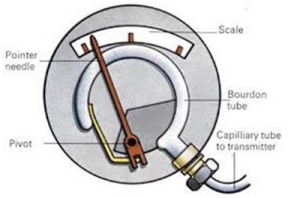
Hackers

Insider Threats

Low power

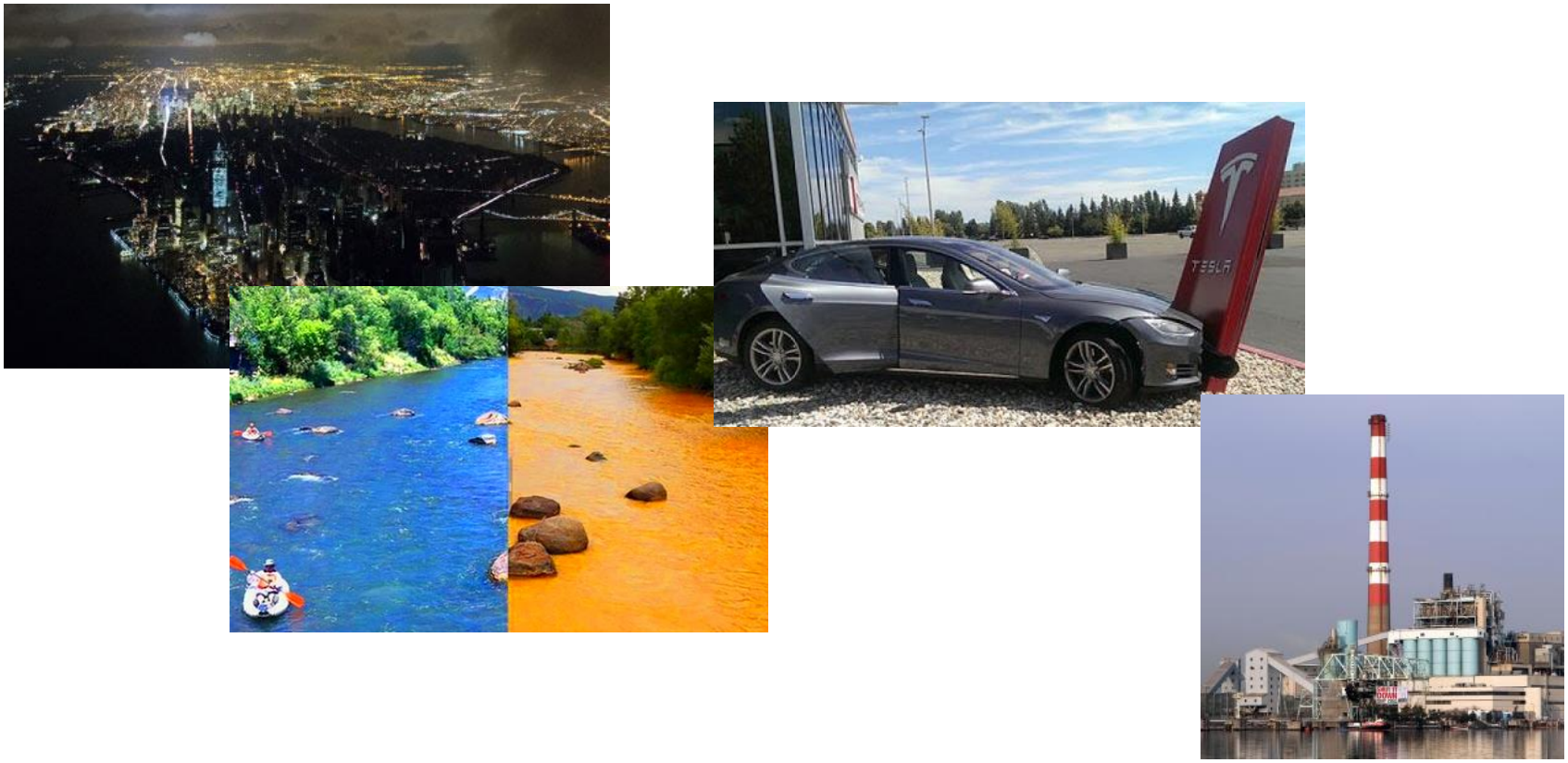


Connectivity Issues



Mechanical Failure

IoT networks are control networks

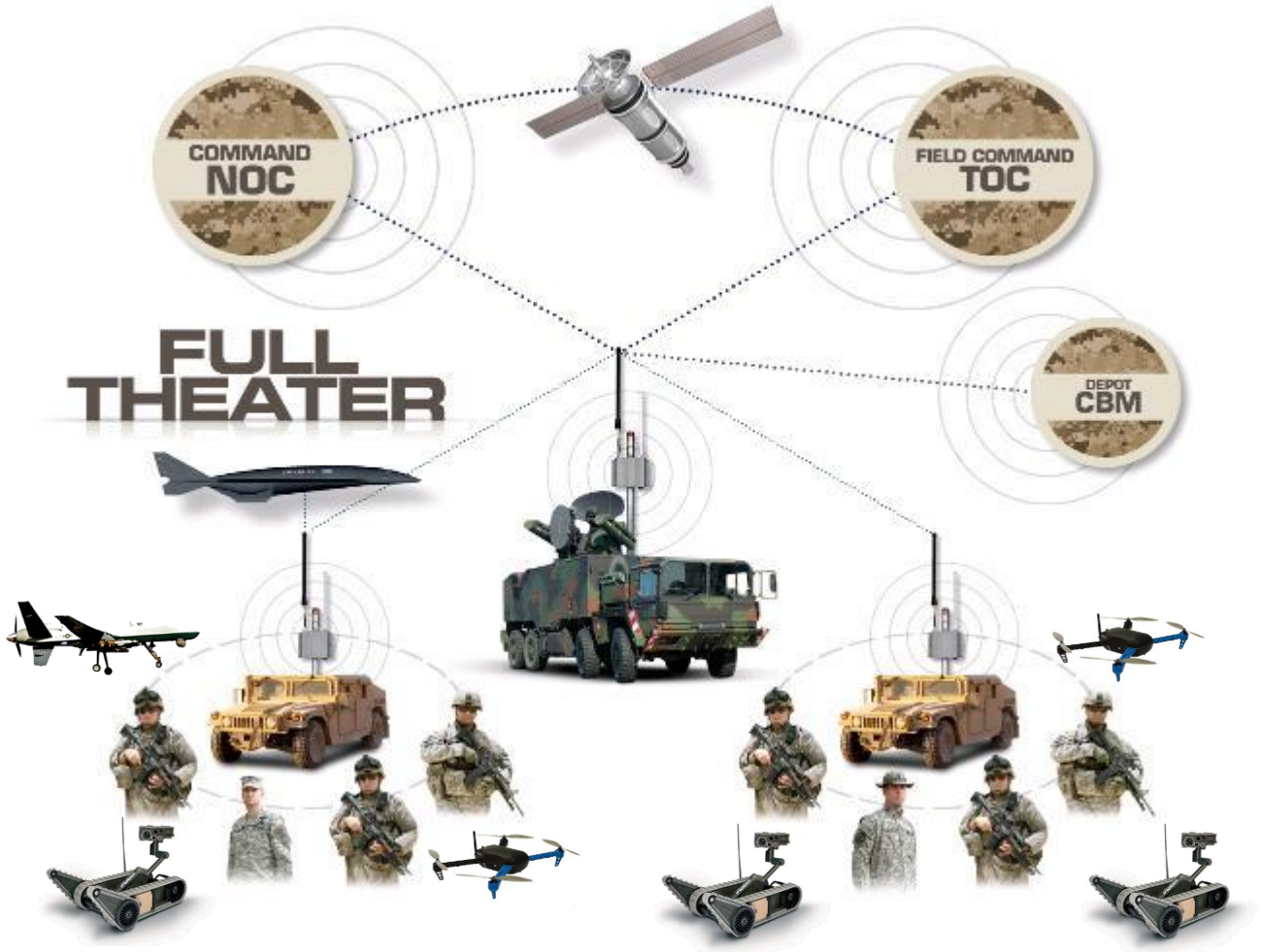


Real-world consequences for failures in IoT networks

How is DARPA involved?

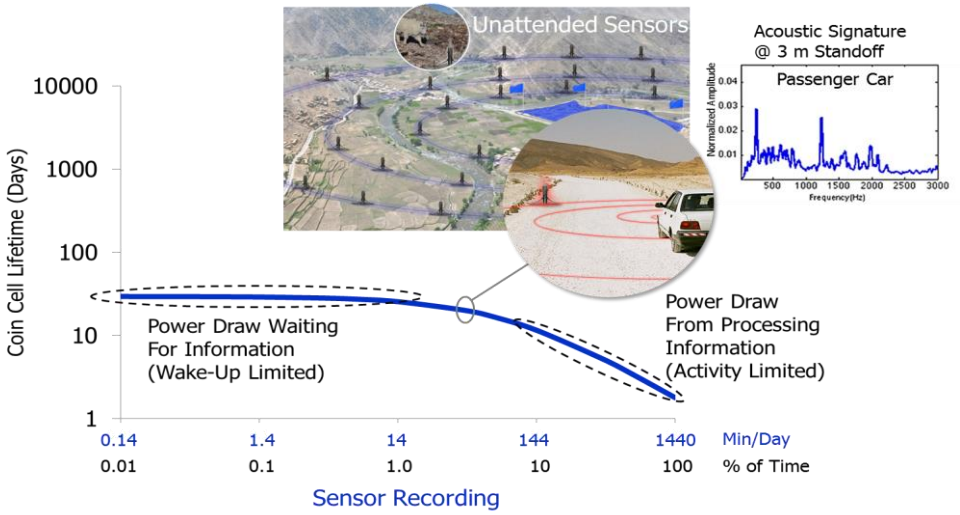
Military faces the same problems

Control/Decision Networks



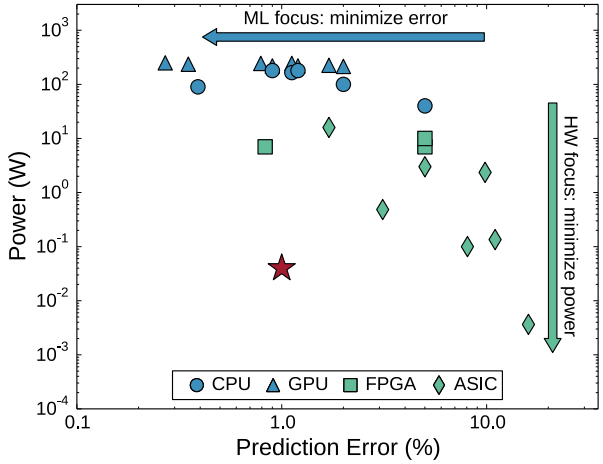
Sensor/Data Networks

Making sensing ubiquitous and smart



<10nW sensing before waking

DNN @ 1000x lower power with best in class accuracy

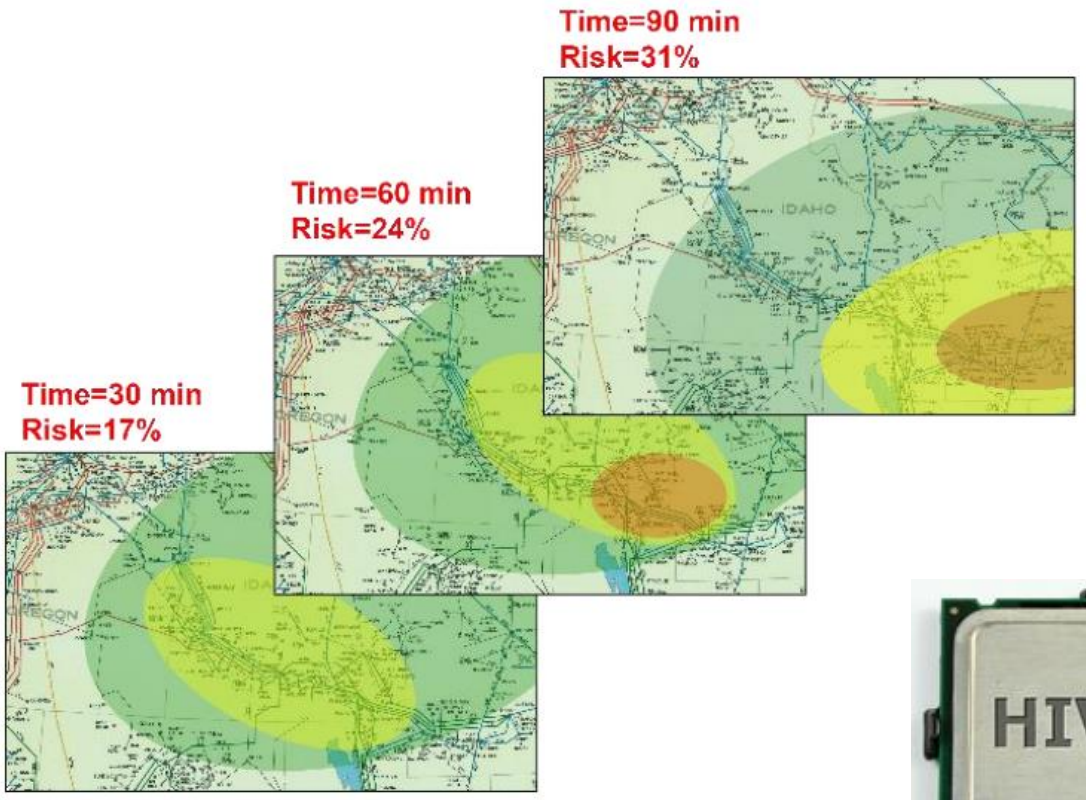


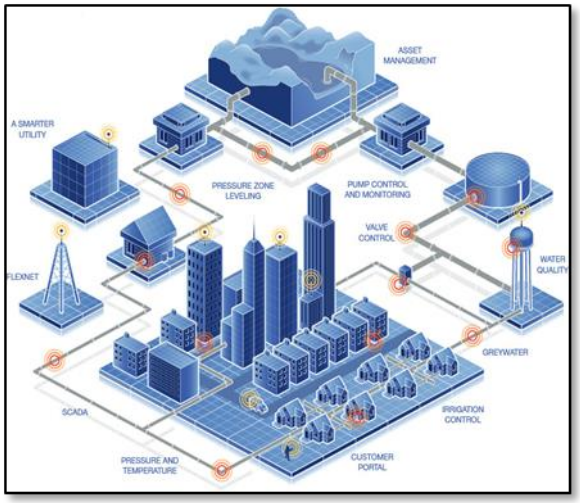
Compression Approach	DNN Architecture	Original Model Size	Compressed Model Size	Reduction in Weights vs. AlexNet	Top-1 ImageNet Accuracy	Top-5 ImageNet Accuracy
None (baseline)	AlexNet [1]	240MB	240MB	1x	57.2%	80.3%
SVD [2] more with less	AlexNet	240MB	48MB	5x	56.0%	79.4%
Network Pruning [3] Delete parameters	AlexNet	240MB	27MB	9x	57.2%	80.3%
Deep Compression [4] Above plus fewer bits	AlexNet	240MB	6.9MB	35x	57.2%	80.3%
None	**SqueezeNet [5] (ours)**	**4.8MB**	**4.8MB**	**50x**	57.5%	80.3%
Deep Compression [4]	**SqueezeNet [5] (ours)**	**4.8MB**	**0.47MB**	**510x**	57.5%	80.3%

510X reduction in weights enables training in the field

[1] A. Krizhevsky, I. Sutskever, G.E. Hinton. ImageNet Classification with Deep Convolutional Neural Networks. NIPS, 2012.
[2] E.L .Denton, W. Zaremba, J. Bruna, Y. LeCun, R. Fergus. Exploiting linear structure within convolutional networks for efficient evaluation. NIPS, 2014.
[3] S. Han, J. Pool, J. Tran, W. Dally. Learning both Weights and Connections for Efficient Neural Networks, NIPS, 2015.
[4] S. Han, H. Mao, W. Dally. Deep Compression..., arxiv:1510.00149, 2015.
[5] **F.N. Iandola**, M. Moskewicz, K. Ashraf, S. Han, W. Dally, K. Keutzer. SqueezeNet: AlexNet-level accuracy with 50x fewer parameters and <1MB model size. arXiv, 2016.

Low power processing to enable edge analytics

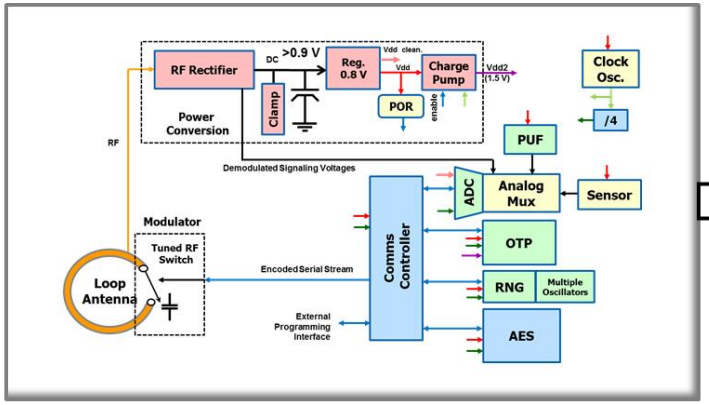




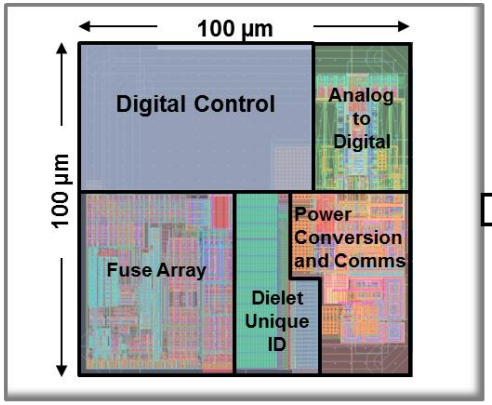
A graph analytics processor with 1000x improvement in processing efficiency

- Relationships between events discovered as they unfold
- Decisions made at the edge of the network

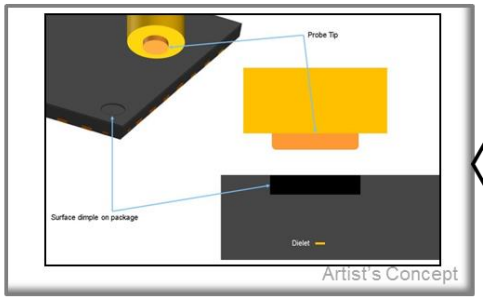
Securing the Internet of Things



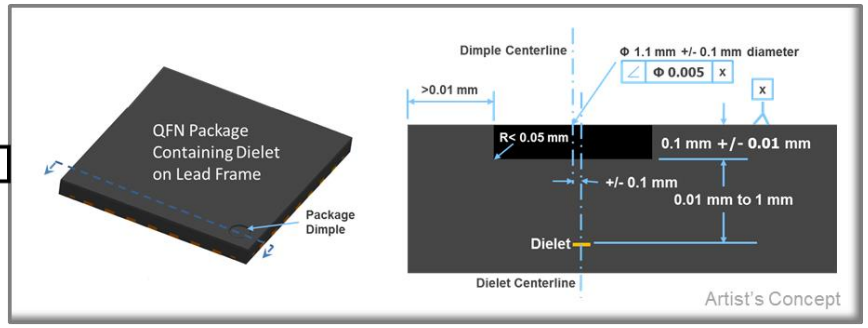
Each SHIELD Dielet contains unique cryptographic Roots of Trust



14nm SHIELD Dielet planned to set record for smallest ASIC ever made



Near Field Reader will be inserted into Package alignment feature to perform SHIELD Dielet authentication



Integrated security for <1¢

How can you get involved?

Commercial engagement and outreach

- Interested in finding industry directions
- Finding common interests
- Working together to advance technologies
  - Google
  - Siri
  - iRobot
  - DARPA Robotics Challenge

Working with DARPA: Flexibility, Speed

Unlike typical government agencies, DARPA can operate in a commercial-like fashion utilizing its ***Other Transactional Authority (OTA).***

- Government rules and regulations for IP, accounting and contract administration do not apply under OTA (i.e. Generally Accepted Accounting Principals (GAAP) are satisfactory).
- An OTA represents a vehicle that is close to a standard business contract, and industry partners don't need to have an expert on government contracting.
- OTA allows DARPA the flexibility to formulate IP arrangements that are mutually beneficial to all parties.

Recent DARPA partnerships

- Intel
- HP
- Motorola
- Nvidia
- 3M
- Xilinx
- Sanofi
- Micron
- Novartis
- Cray Research, Inc.

Areas of interest for DARPA/MTO

- Cyber Resiliency
  - Authentication
  - Access control
  - Information assurance
- Low power and remote sensors
  - Physical security
  - Power delivery
  - Connectivity
  - Cost
  - Ruggedized systems
- Decision making and control
  - Sensor fusion
  - Sensor tasking
  - Automation

Got an idea? Contact us

- Trung Tran, DARPA/MTO Program Manager (trung.tran@darpa.mil)
  - Nicole Heidel (nicole.heidel.ctr@darpa.mil), SETA
  - Mark Laurri (mark.laurri.ctr@darpa.mil), SETA

IEEE Proceedings Special Issue on IoT

- DARPA is currently soliciting contributors (U.S. and International) for an upcoming Proceedings of the IEEE Special Issue on IoT Security
  - Authentication and encryption in IoT devices
  - Security in autonomous vehicles
  - Smart Cities
  - Security in industry/factory floor
  - Test Beds
- Each of the survey-style papers (10-12 pp. in length) should include the following:
  - IoT foundations
  - State-of-the-art
  - Challenges
  - Outlook
- Anticipated publication date: Fall 2017